	POLICY#	STATUS	ISSUED	LAST REVISED	PAGE
	10-01		2/17/07	7/21/06	1 of 6
State of Rhode Island Department of Administration Division of Information Technology		TITLE	Enterprise Password Security		

1.0 Policy Statement:

Employees and vendors accessing State of RI information resources who use password authentication shall use a password that complies with this policy.

2.0 Policy Objective:

Ensure that State of RI information resources are protected by passwords that are secure and selected to hinder unauthorized access to password-protected resources.

3.0 Definitions:

State Employee: Any employee of the State of Rhode Island performing services within the executive department except any person:

- 1) Who has been employed less than 6 months; or
- 2) Who is a temporary, seasonal or on-call employee.


State Agency: Any department, commission, board, office, or other agency that:

- 1) is in the executive of state government;
- 2) has authority that is not limited to a geographical portion of the state; and
- 3) was created by the constitution or a statute of this state.

4.0 Policy and Control Requirements:

4.1 Compliant Activities:

- Each employee shall have a unique user identification (User ID) and password.
- Employees shall assign their own passwords.
- Passwords shall be changed (at least) every 90 days.
- Passwords shall contain a minimum of 8 characters.
- Passwords shall include a combination of at least 3 of the following 4 types: alphabetic, numeric, special characters, both upper and lower case.
- Passwords shall be changed after first assignment or following a password reset.

	POLICY#	STATUS	ISSUED	LAST REVISED	PAGE
	10-01				
State of Rhode Island Department of Administration Division of Information Technology	TITLE	Enterprise Password Security			

- Passwords shall be encrypted while stored on the computer.
- Passwords shall be changed as soon as they expire.
- Accounts shall be locked out after three unsuccessful login attempts.
- Passwords shall not be duplicated within the last 15 occurrences (changes).
- Employees shall change passwords when advised of a potential security breach by the Chief Information Security Officer (CISO), CISO's designee or agency information security manager.

4.2 Permitted Activities:

- Password defaults can be used for initial hardware and software setup or configuration. Following initial activities, these defaults shall be changed.
- Expired passwords shall be used only to reset or to self-assign a new password.

4.3 Prohibited Activities

- Passwords shall not contain the User ID, user name, company name, replicated sequence of characters, or any complete dictionary words.
- Passwords and User IDs shall not be provided to others or shared.
- Passwords and User IDs shall not be posted or displayed where other individuals may have access.


5.0 Exceptions to Policy:

Exceptions to this policy may be granted solely by the CISO or the CISO's designee.

Examples of possible exceptions that may be permitted:

- Passwords for special use and restricted accounts such as training or service accounts may be defined to not expire, shared, etc.
- Passwords may be included in secured batch files only if no other acceptable alternative can be identified.
- Password complexity requirements may be adjusted to suit older legacy hardware and software in instances where meeting the full requirements of this policy would either be impossible or cost-prohibitive.

6.0 Password Resets

	POLICY#	STATUS	ISSUED	LAST REVISED	PAGE
	10-01		2/17/07	7/21/06	3 of 6
State of Rhode Island Department of Administration Division of Information Technology	TITLE	Enterprise Password Security			

An employee can request to have his/her password reset for central administrative systems hosted and administered by Division of Information Technology in two ways.


6.1 Visit the Service Desk

- 6.1.1 Complete the attached Reset Password Request form to have their password reset.
- 6.1.2 The Service Desk will request the requesting party to verify their identity via a State Id or Drivers license.
- 6.1.3 Once verification has been completed the Service Desk will built a service ticket a forward the ticket to the appropriate service queue for action. (24 hour response is guaranteed)
- 6.1.4 Service desk will reset the password to allow user access to the network. A message will be left on the user's voice mail with new password.

6.2 Telephone the Service Desk

- 6.2.1 Complete the attached Reset Password Request form to have their password reset.
- 6.2.2 Fax completed form to Service Desk at (401 222-3151) and follow-up with a call to (401) 222-5709. The Service Desk will confirm receipt of form and verify all information.
- 6.2.3 Once verification has been completed the Service Desk will built a service ticket a forward the ticket to the appropriate service queue for action. (24 hour response is guaranteed)
- 6.2.4 Service desk will reset the password to allow user access to the network. A message will be left on the user's voice mail with new password.

7.0 Implementation Responsibility:

	POLICY#	STATUS	ISSUED	LAST REVISED	PAGE
	10-01				
State of Rhode Island Department of Administration Division of Information Technology	TITLE	Enterprise Password Security			

Each employee shall be responsible for selecting a secure password, maintaining password confidentiality, and promptly changing the password when any security breach is suspected. The RI DOIT member shall review security logs regularly to identify suspicious login attempts or recurring failures.

Any individual requesting an employee password shall be referred to this policy document, the agency manager, or to the CISO or the CISO's designee.

8.0 Compliance Responsibility:

State Agencies shall be responsible for implementing and enforcing the Password Security Policy within their supported areas.

State Agency managers shall be responsible for ensuring that employees who report to them comply with this policy.


10.0 Policy Violations and Disciplinary Actions:

An employee found to be in violation of this policy may face disciplinary action up to and including dismissal from employment and/or criminal prosecution where the act constitutes a violation of law. A breach of contract, where applicable, may also be considered.

11.0 References:

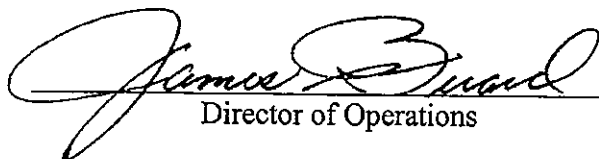
HIPAA 164.310 Physical Safeguards
 (c) Workstation Security
 HIPAA 164.312 Technical Safeguards
 (a) (1) Access Control
 (2) Implementation Specifications
 (i) Unique User Identification
 (ii) Emergency Access Procedure
 (iii) Automatic Logoff
 HIPAA 164.312 (d) Person or Entity Authentication
 Cross-reference Access Security Policy

12.0 Approvals:

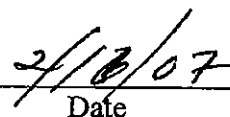
	POLICY#	STATUS	ISSUED	LAST REVISED	PAGE
	10-01				
State of Rhode Island Department of Administration Division of Information Technology		TITLE	Enterprise Password Security		

Assistant Director of Planning, Policy & Technology

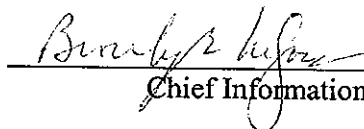
Date



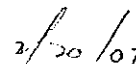
Director of Operations



Date




Chief Information Officer



Date

Director, Department of Administration

Date

	POLICY#	STATUS	ISSUED	LAST REVISED	PAGE
	10-01				
State of Rhode Island Department of Administration Division of Information Technology		TITLE	Enterprise Password Security		

Password Reset Request Form	
Account to be reset:	
Date:	
User Name:	
Phone Number:	
Department:	
Employee ID Badge No.:	
Signature:	

I _____ (print name of supervisor) as the supervisor of the above named employee, authorize to have his/her password reset.

Signed _____ Date: _____